RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: CSO-M01

What Directors and CISOs Need to Know About Cyber Mandates for AI Systems

MODERATOR:

Scott M. Giordano, Esq.
Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/scottmgiordano

PANELISTS:

John Barker, Esq., CHC, CCEP, CHPC, CHRC
Partner
The CISO Law Firm PLLC
linkedin.com/in/johnwbarkerii

David Patariu, Esq., PLS, CISSP
Partner
The CISO Law Firm PLLC
linkedin.com/in/dpatariu

John G. Bates, JD, AIGP, CISSP, CCSP
Senior Manager, Cybersecurity
Ernst & Young LLP
linkedin.com/in/john-bates-jd

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The information shared during this panel discussion is for general informational purposes only and does not constitute legal advice. No attorney-client relationship is formed by attending or participating in this discussion. The views expressed by the panelists are their own and do not necessarily reflect the opinions of their respective law firms, clients, or any affiliated organizations.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. The views expressed by the presenters are their own and not necessarily those of Ernst & Young LLP or other members of the global EY organization or The CISO Law Firm. These slides are for educational purposes only and are not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice. SCORE no. 26447-251US_2

The Panel

MODERATOR:

Scott M. Giordano, Esq.

Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/scottmgiordano

PANELISTS:

John Barker, Esq.

Partner
The CISO Law Firm PLLC
linkedin.com/in/johnwbarkerii

David N. Patariu, Esq.

Partner
The CISO Law Firm PLLC
linkedin.com/in/dpatariu

John Bates, JD

Senior Manager, Cybersecurity
Ernst & Young LLP
linkedin.com/in/john-bates-jd

Agenda

01

Why this matters

02

Overview of artificial intelligence (AI) regulations and cybersecurity mandates

03

AI governance strategies and best practices

04

Cybersecurity threats to AI models

05

AI governance project plan

RSAC 2025 Conference

Why this matters

Key paradigms

Capital investment in AI is immense.

Cybersecurity threats against AI systems are novel, sophisticated and developing.

Governments are implementing regulations covering AI implementation, maintenance, testing, documentation and registration.

Cyber must balance AI risk with supporting the speed of business.

Cyber and Legal must determine a reasonable security program.

Organizations that fail to comply with these regulations may face legal penalties, financial loss and/or reputational damage.

Source:
https://seo.ai/blog/deepseek-users-downloads

RSAC 2025 Conference

Overview of AI regulations

US AI regulations: federal

Biden Executive Order 14110 (2023) – Focuses on safe, secure, and trustworthy AI development

National Institute of Standards & Technology (NIST) AI Risk Management Framework (2023): Security Guidelines for AI systems

AI-specific enforcement actions by the US Securities and Exchange Commission (SEC), Department of Justice (DOJ) and Federal Trade Commission (FTC)

Trump Executive Order: Removing Barriers to American Leadership in Artificial Intelligence (January 23, 2025)

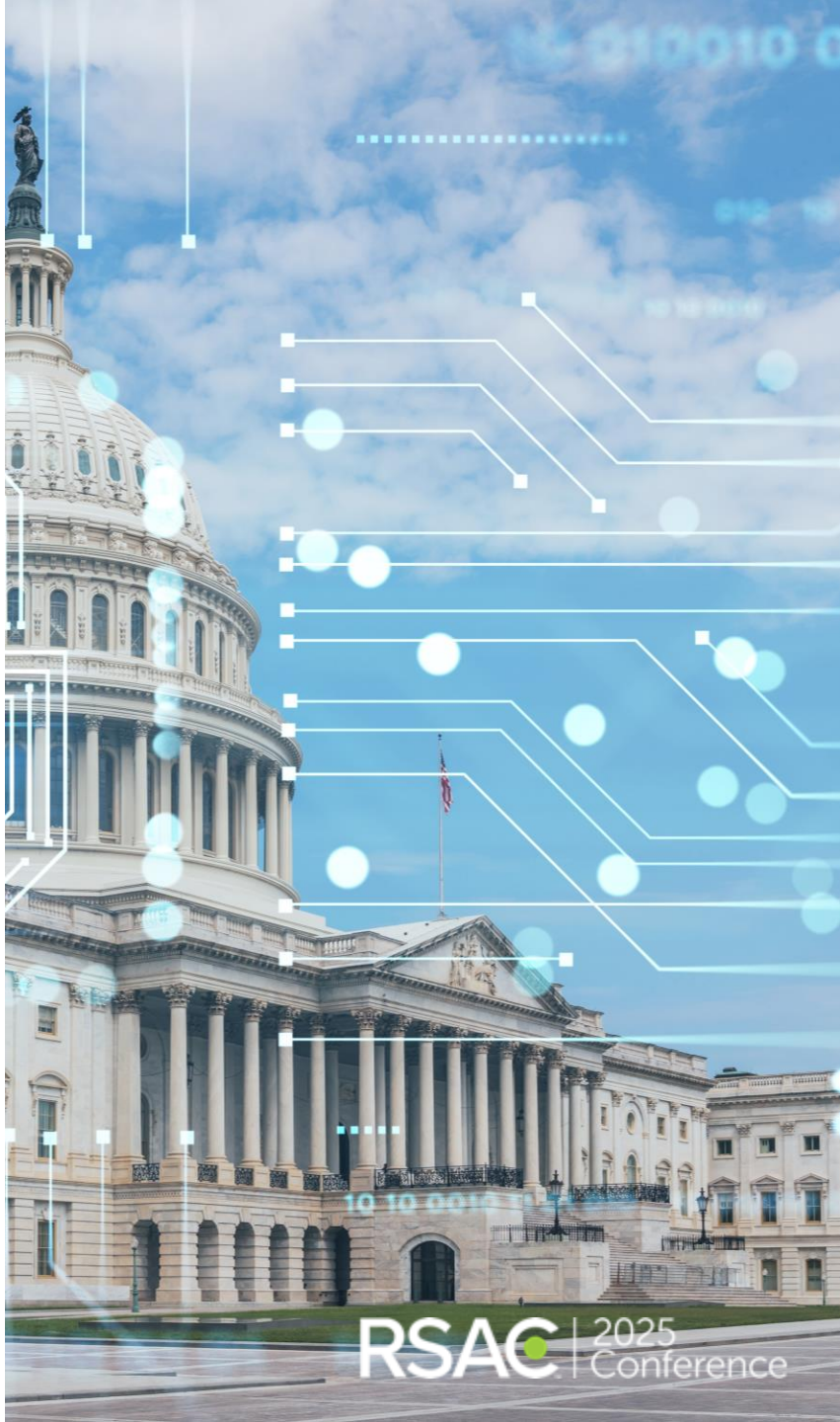
US AI regulations: federal

Biden Executive Order 14110 (2023) – Focuses on safe, secure, and trustworthy AI development

National Institute of Standards & Technology (NIST) AI Risk Management Framework (2023): Security Guidelines for AI systems

AI-specific enforcement actions by the US Securities and Exchange Commission (SEC), Department of Justice (DOJ) and Federal Trade Commission (FTC)

Trump Executive Order: Removing Barriers to American Leadership in Artificial Intelligence (January 23, 2025)



State AI laws overview

California	Colorado	Utah
Focus: 18+ laws addressing AI across sectors: automated decision-making, data privacy, deepfakes, AI-generated clones of deceased actors and government AI use.	**Focus:** Targets algorithmic discrimination in "high-risk AI systems" impacting consequential decisions (employment, lending, health care)	**Focus:** Promotes responsible AI deployment in the private sector while avoiding excessive regulation
Deployers: (1) Disclose use of generative AI (GenAI) in health care communications and (2) ensure licensed physicians oversee AI in healthcare	**Deployers:** (1) Risk management and algorithmic impact assessments; (2) disclosure to consumers; (3) consumers can appeal adverse decisions	**Deployers:** (1) Clear disclosure to consumers when interacting with GenAI; (2) special focus on disclosure in health care and dentistry
Developers: (1) Transparency in AI training data; (2) disclose AI data sources; (3) disclose use of copyright or licensed data in training	**Developers:** Provide info/documents to deployers to fulfill responsibilities and mitigate algorithmic discrimination	**Developers:** Compliance with disclosure obligations and ensuring AI technologies meet regulatory standards for professional contexts
Enforcement: California Attorney General and agencies have enforcement power, including risk analyses. Limited private rights of action for damages, injunctive relief, and equitable relief for deepfakes and digital replicas	**Enforcement:** Colorado Attorney General has broad enforcement power and can pass regulations. Affirmative defense against CO AI via ISO 24001/NIST AI Act.	**Enforcement:** Division of Consumer Protection has authority to impose fines and seek court remedies for violations

SEC, FTC and DOJ regulatory actions

SEC has initiated several lawsuits regarding "AI-washing"

SEC "material affect" breach notifications resulting from AI models

FTC has authority over any product being marketed to the public or related to commerce

Overstating the ability or "magic" of an AI product

Privacy notices that AI is being utilized and potential opt-out

Federal regulators call this "old school fraud using new school buzzwords like 'artificial intelligence' and 'automation'"

Source:
https://www.naag.org/attorney-general-journal/a-deep-dive-into-colorados-artificial-intelligence-act/
https://en.wikipedia.org/wiki/Colorado

Global Regulatory Overview

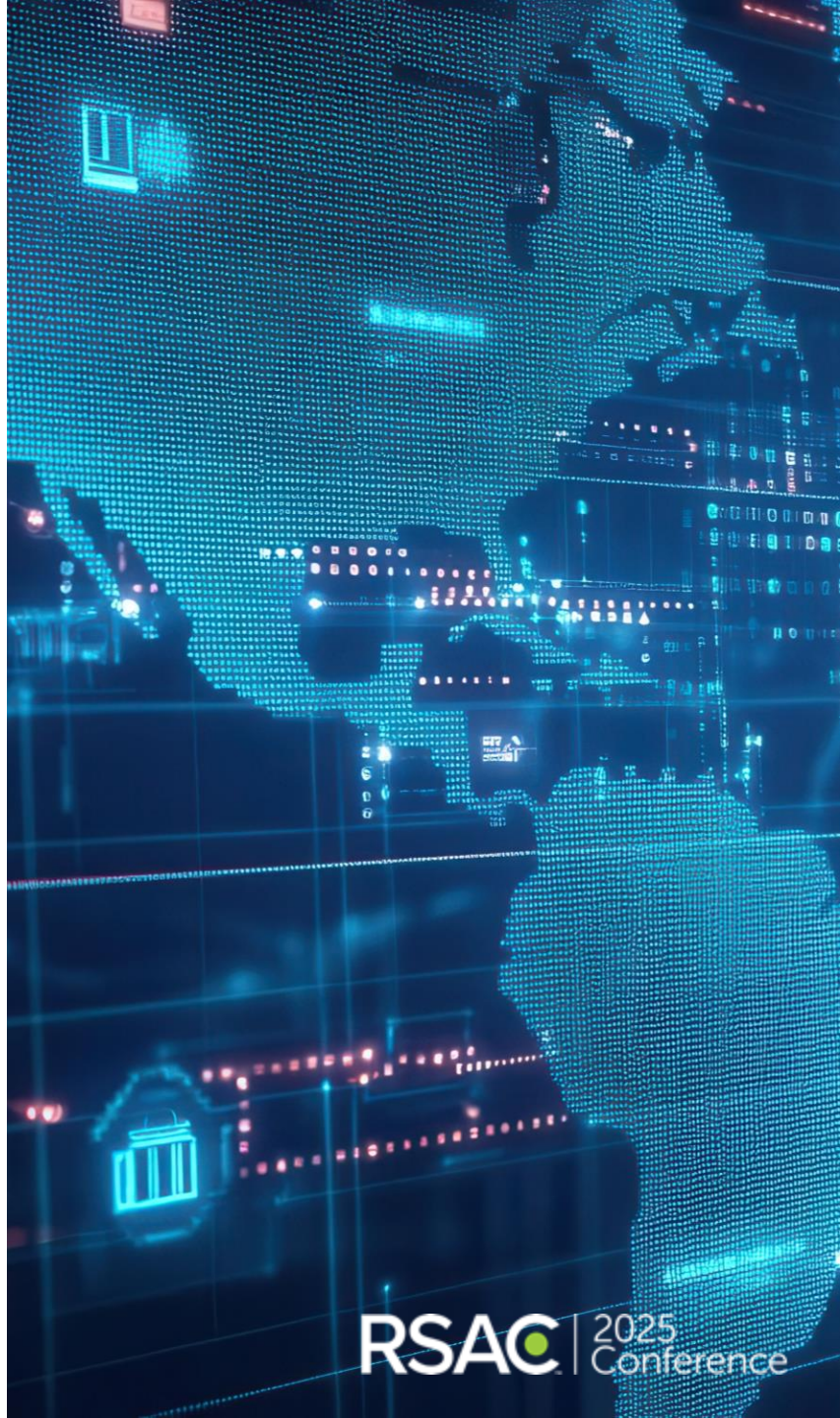
European Union (EU) AI Act: categorizes AI risks and mandates security measures

China’s AI security regulations: focuses on algorithmic transparency and government oversight

EU Global Data Protection Regulation (GDPR): protects personal data processed

Singapore: sector guidance and economic growth

OECD and United Nations guidelines: promotes global AI safety standards



EU AI Act classification schema

RISK TIER

Unacceptable risk to rights or safety Art 5

OBLIGATIONS

Prohibited except in certain emergencies

EXAMPLES

Social scoring by governments, real-time biometric ID, behavioral manipulation but can be allowed in national defense and security, military, war and national emergency

RISK TIER

High risk to rights or safety Article 6

OBLIGATIONS

Allowed under stringent conditions/risk management requirements

EXAMPLES

Critical and digital infrastructure, government services, biometric (not real-time), insurance, health, job interviews and resumes

RISK TIER

Limited risk to rights or safety Article 52

OBLIGATIONS

Transparency requirements

EXAMPLES

AI applications that make it possible to generate or manipulate images, sounds or videos (deepfakes)

RISK TIER

Minimal risk to rights or safety Article 69

OBLIGATIONS

Voluntary

EXAMPLES

Anti-spam filters, video games that use AI for images, sounds, video and more

https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

EU AI Act requirements

Overall

01
Design and development requirements

02
Resilience against attacks

03
Incident reporting obligations

04
Technical documentation and recordkeeping

05
Post-market monitoring

06
Data governance and management

Specific cyber requirements

01
Must achieve consistent accuracy, robustness and cybersecurity across entire AI lifecycle

02
Technical solutions must address:

- Third-party exploitation of system vulnerabilities
- Training data attacks: data poisoning and model poisoning
- Input attacks: adversarial examples, model evasion, confidentiality attacks and exploitation of model flaws

RSAC 2025 Conference

AI governance strategies and best practices

Cyber program challenges

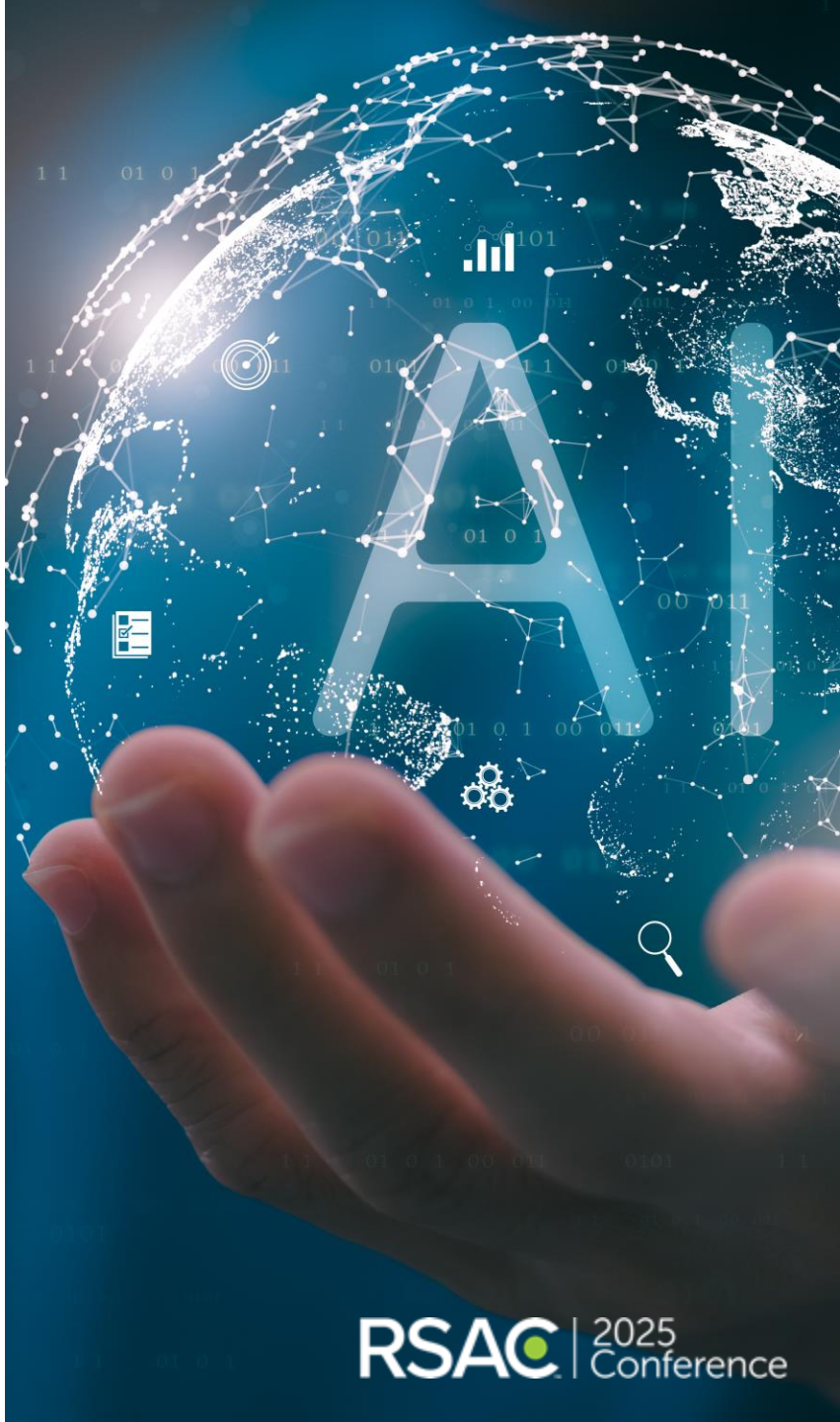
AI governance will be impeded by the following

- Incomplete configuration management database (CMDB)
- Ineffective vendor management/procurement practices (shadow IT)
- Lax data governance, especially data labeling and deletion
- Generic cyber training and education
- Lack of cross-functional success between legal, cyber, privacy, data science, IT and the business
- Immature disaster recovery (DR) and business continuity planning

Source:
https://seo.ai/blog/deepseek-users-downloads

APPLY: implementing AI governance

- Augment current compliance processes (e.g., Third Party Risk Management (TPRM), Architecture Review Board (ARB), Privacy)
- Shift away from determinative cyber threat modeling and solutioning
- Educate and train all operations what is AI and what is ML
- Update CMDB and Incident Response/Crisis Management Plans
- Create new documentation (model cards) with constant testing
- Risk rank AI solutions (LLM model vs. SaaS with “AI”)
- Develop AI Governance policies aligned with NIST AI RMF or ISO 42001 frameworks
- Cross-functional collaboration by engaging legal, security, privacy, data science, ethics, and engineering teams



APPLY: best practices

Contemplate a holistic corporate approach to utilizing AI throughout the enterprise (i.e., using the same base agents) to avoid sprawl

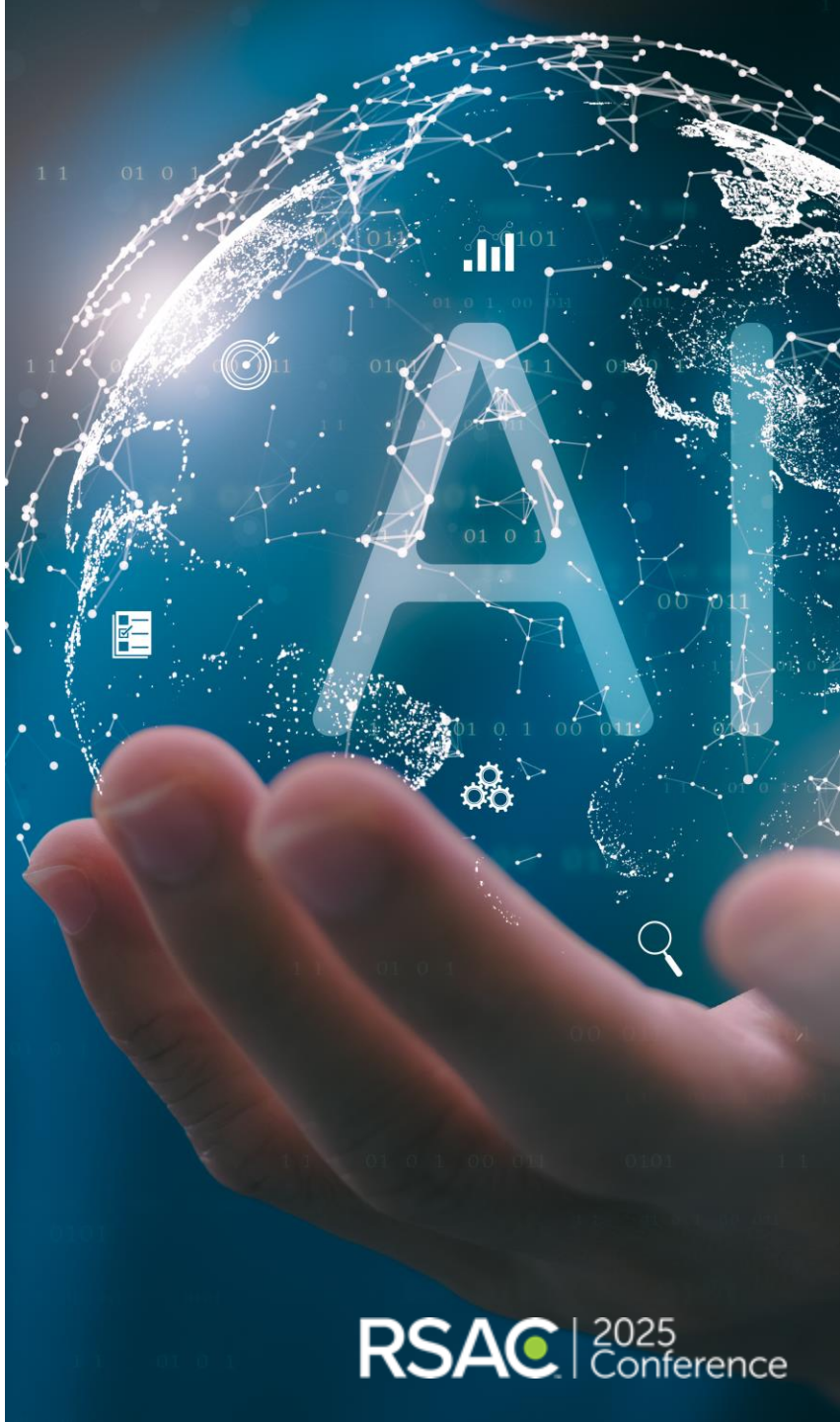
Build coalition of Cyber, Legal, Privacy, TPRM, Data Science, Sales/Marketing, Ethics, Internal Audit, Architecture, DR and Finance

Differentiate between critical AI systems and SaaS with AI

Determine single corporate AI governance framework/approach

Determine how to address the novel AI risks (e.g., “overreliance”)

Create a simple risk matrix with different levels of AI review



RSAC 2025 Conference

Cybersecurity threats to AI models

AI threat modeling

OveraLLM applications 2025

01 Prompt injection	**02** Sensitive information disclosure
03 Supply chain	**04** Data and model poisoning
05 Improper output handling	**06** Excessive agency
07 System prompt leakage	**08** Vector and embedding weaknesses
09 Misinformation	**10** Unbounded consumption

MITRE ATLAS

14	91	26
TACTICS	TECHNIQUES	MITIGATIONS

01 Reconnaissance	**02** Resource and development
03 Initial and access	**04** ML model access
05 Execution	**06** Persistence
05 Privilege and escalation	**06** Defense and evasion

Agentic AI threat modeling

Cloud Security Alliance (CSA) MAESTRO

01
Foundation models

02
Data operations

03
Agent frameworks

04
Deployment and infrastructure

05
Foundation models

06
Data operations

07
Evaluation and observability

08
Security and compliance

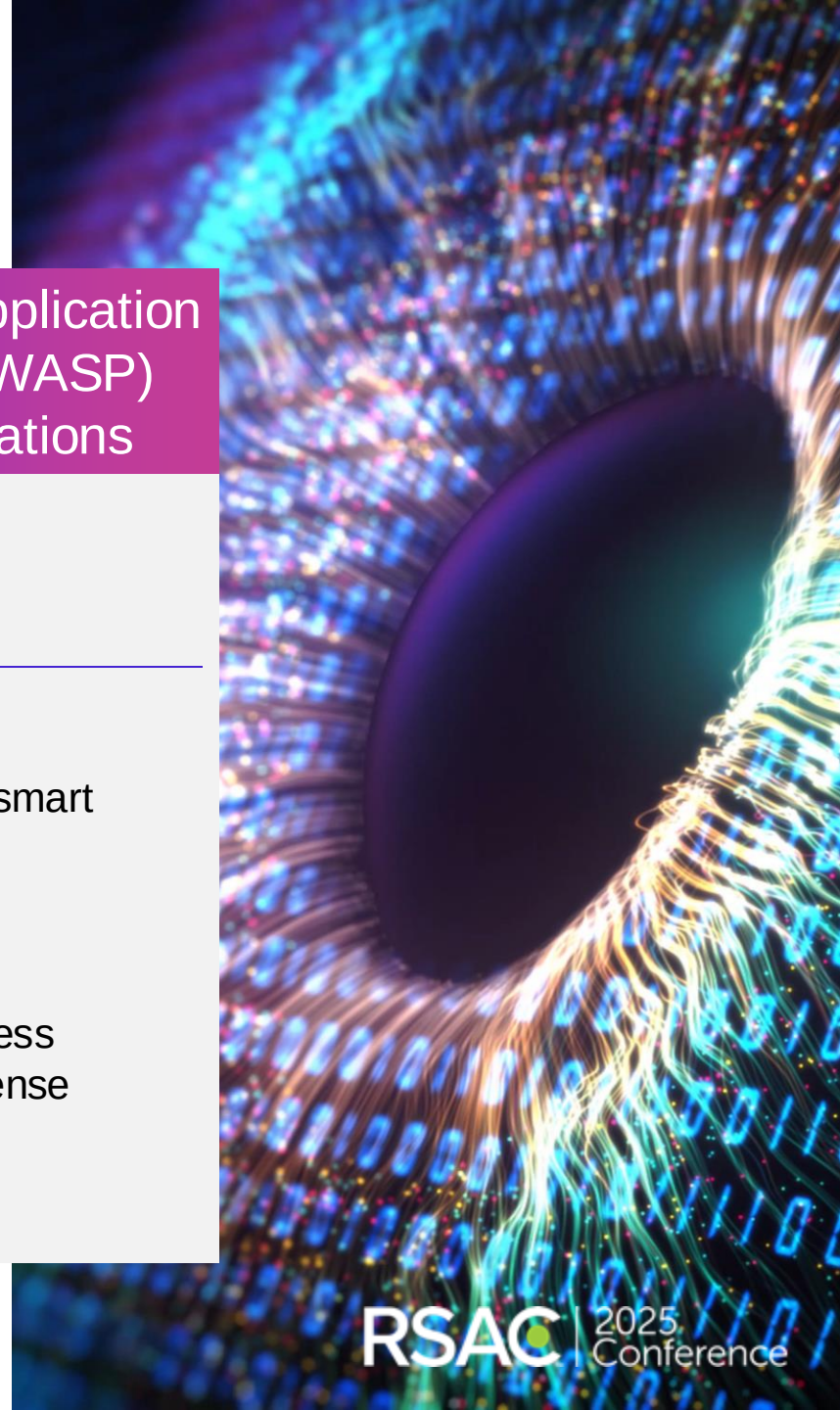
09
Agent ecosystem

Open Worldwide Application Security Project (OWASP) AI threats and mitigations

01
Enterprise Co-pilots

02
Internet of things (IoT) in smart home security cameras

03
Agent-driven robotic process automation (RPA) in expense reimbursement



OWASP LLM Exploit Generation v1.0

Examines ability of LLMs to exploit vulnerabilities in OWASP Juice Shop

Tested GPT-4o, Claude and DeepSeek r-1

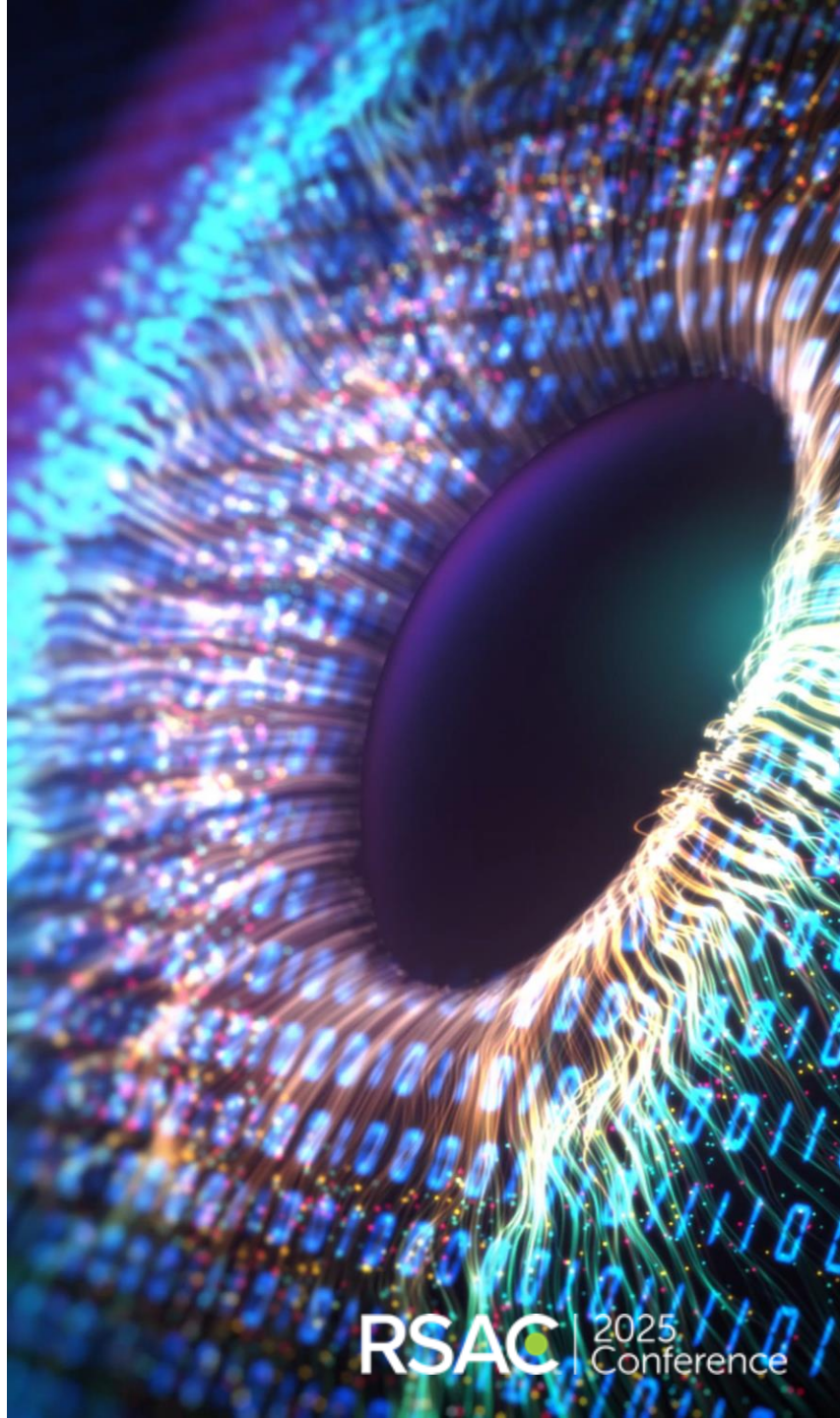
Initial findings

Not stealthy – noisy and would be detected

Requires access to advanced models and infrastructure – DeepSeek failed

Resource efficiency – it is expensive

Success detection limitations – could not determine exploitation



APPLY: securing AI

- Augment current cloud security practices
- Implement controls to prevent lateral movement of data
- Label, restrict, monitor and delete data throughout enterprise
- Deploy continual adversarial testing
- Continuous monitoring and logging of model inputs and outputs
- Restrict access to data moving in and out of AI solutions
- Educate employees on AI and emerging risks
- Investigate new solutions to detect, document and defend

RSAC 2025 Conference

Project plan

Where to start?

01
Determine business AI strategy and approach

02
Establish AI governance with Cyber and Legal

03
Integrate into enterprise risk management (ERM) with corporate risk appetite

04
Create an AI inventory (model vs. SaaS)

05
Draft policies and procedures

06
Document day-to-day operations (Responsible, Accountable, Consulted, Informed (RACI))

07
Define continuous evaluation, testing, and remediation approach (US DOJ compliance program guidance)

08
Customized training and education

09
Repeat (ISO approach)

RSAC 2025 Conference

Conclusions

Conclusions and key takeaways

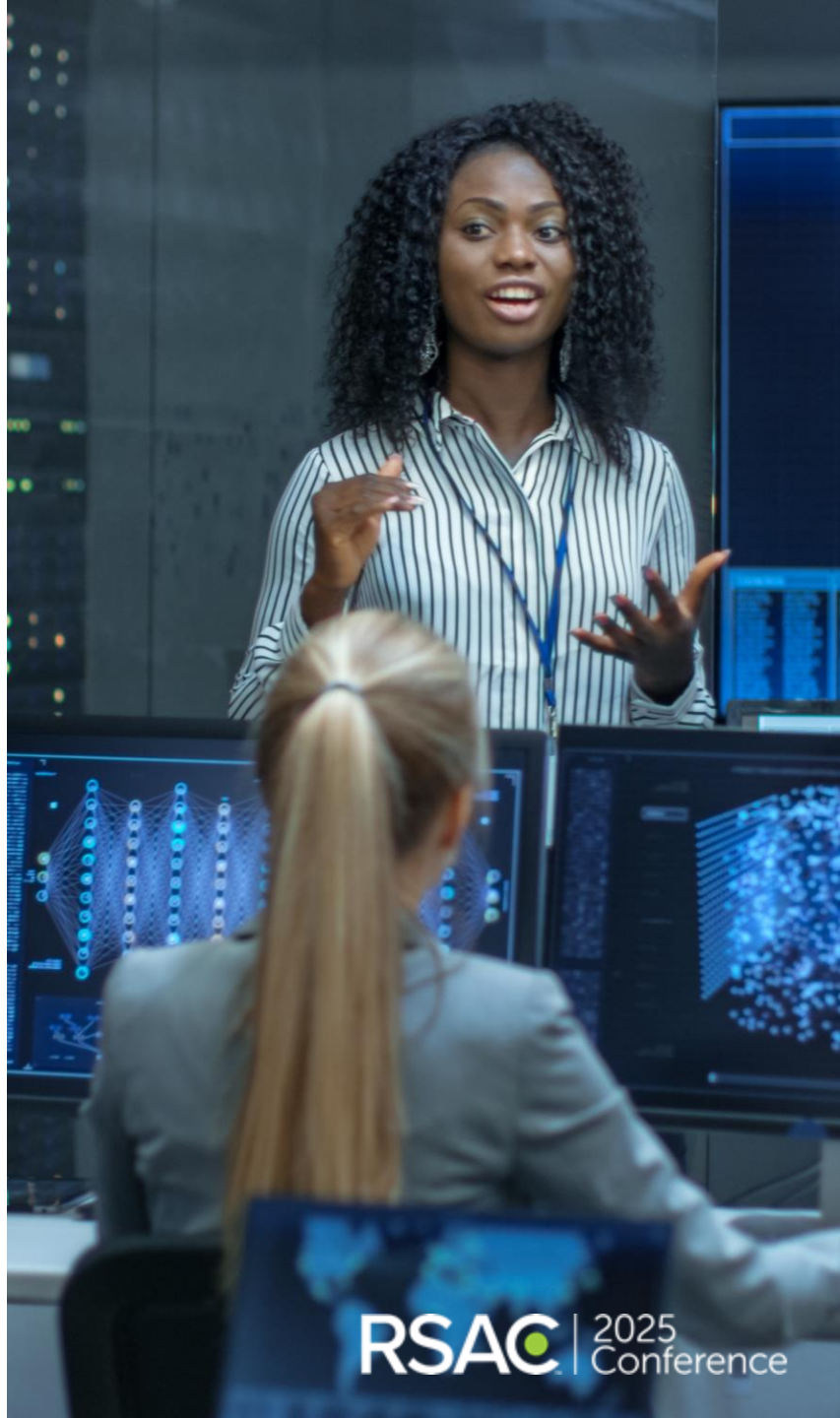
AI cybersecurity is a growing concern requiring proactive strategies.

Compliance is evolving, and organizations must stay ahead of the regulations.

Governance, risk management and monitoring are key (Cybersecurity + Legal).

Neglected practices (data governance (DG), CMDB, vendor management, access controls, data loss prevention (DLP)) will challenge AI governance.

Governance needs to support the speed of business, otherwise shadow IT and higher-risk behaviors will flourish.



References

California's AI laws

- AB-1831 Crimes: child pornography. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1831
- SB-926 Crimes: distribution of intimate images. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB926
- SB-981 Sexually explicit digital images. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB981
- AB-2602 Contracts against public policy: personal or professional services: digital replicas. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2602
- AB-1836 Use of likeness: digital replica. @ https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1836
- AB-2655 Defending Democracy from Deepfake Deception Act of 2024. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2655
- AB-2839 Elections: deceptive media in advertisements. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2839
- AB-2355 Political Reform Act of 1974: political advertisements: artificial intelligence. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2355
- AB-2013 Generative artificial intelligence: training data transparency. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2013
- AB-3030 Health care services: artificial intelligence. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB3030
- SB-1120 Health care coverage: utilization review. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1120
- SB-1223 Consumer privacy: sensitive personal information: neural data. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1223
- AB-1008 California Consumer Privacy Act of 2018: personal information. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1008

References

California's AI laws (continued)

- SB-942 California AI Transparency Act.(2023-2024). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1008
- AB-2905 Telecommunications: automatic dialing-announcing devices: artificial voices. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2905
- SB-896 Generative Artificial Intelligence Accountability Act. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB896&utm_source=chatgpt.com
- AB-2876 Pupil instruction: media literacy: artificial intelligence literacy: curriculum frameworks: instructional materials. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2876&utm_source=chatgpt.com
- AB 2885 Artificial Intelligence. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2885
- SB-1288 Public schools: artificial intelligence working group. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB1288

References

- Colorado AI Act https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf
- Utah AI Policy Act https://le.utah.gov/~2024/bills/static/SB0149.html
- Virginia High-Risk Artificial Intelligence Developer and Deployer Act https://lis.virginia.gov/bill-details/20251/HB2094/text/HB2094 (awaiting signature by governor as of 03/22/2025)
- EU AI Act https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- NIST AI RMF 1.0 https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
- NIST CSF 2.0 https://www.nist.gov/cyberframework
- NIST RMF https://csrc.nist.gov/projects/risk-management/about-rmf
- Executive Order: REMOVING BARRIERS TO AMERICAN LEADERSHIP IN ARTIFICIAL INTELLIGENCE https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
- Cloud Security Alliance MAESTRO https://cloudsecurityalliance.org/blog/2025/02/06/agentic-ai-threat-modeling-framework-maestro
- OWASP Generative AI Security Project https://genai.owasp.org/
- OWASP Juice Shop https://atlas.mitre.org/
- MITRE ATLAS https://atlas.mitre.org/
- Responsible, Accountable, Consulted, Informed (RACI) https://en.wikipedia.org/wiki/Responsibility_assignment_matrix
- US DOJ Compliance Program Guidance https://www.justice.gov/criminal/criminal-fraud/compliance

THANKS!

MODERATOR:

Scott M. Giordano, Esq.

Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/scottmgiordano

PANELISTS:

John Barker, Esq.

Partner
The CISO Law Firm PLLC
linkedin.com/in/johnwbarkerii

David N. Patariu, Esq.

Partner
The CISO Law Firm PLLC
linkedin.com/in/dpatariu

John Bates, JD

Senior Manager, Cybersecurity
Ernst & Young LLP
linkedin.com/in/john-bates-jd

RSAC 2025 Conference

Many Voices.
One Community.

The End